

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Петренко Вячеслав Иванович
Должность: и.о. директора Института цифрового развития
Дата подписания: 28.02.2024 10:35:54
Уникальный идентификатор документа:
b47f96eea65a162179f94dbf7f50b10000a/ad4d

Наименование дисциплины	Аннотация дисциплины Управление информационной безопасностью
Краткое содержание	Введение. Важность и актуальность дисциплины. Ее взаимосвязь с другими дисциплинами специальности. Содержание дисциплины. Виды контроля знаний. Базовые вопросы управления ИБ. Сущность и функции управления. Наука управления. Принципы, подходы и виды управления. Цели и задачи управления ИБ. Понятие системы управления. Стандартизация в области управления ИБ. Стандартизация в области построения систем управления. История развития. Существующие стандарты и методологии по управлению ИБ: их отличия, сильные и слабые стороны (на примере семейства стандартов ISO/IEC 2700x, СТО БР ИББС-1.0, ГОСТ Р ИСО/МЭК 17799, ГОСТ Р ИСО/МЭК 27001, ISO/IEC 18044, BS 25999 и др.). Системы управления ИБ. Процессный подход. Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Понятие процессного подхода. Процессный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления (на примере СУИБ). Понятие СУИБ. Место СУИБ в рамках общей системы управления предприятием. Основные процессы СУИБ и требования, предъявляемые к ним каждым из стандартов. Область деятельности СУИБ. Понятие области деятельности СУИБ. Механизм выбора области деятельности. Состав области деятельности (процессы, структурные подразделения организации, кадры). Описание области деятельности (структура и содержание документа). Ролевая структура СУИБ. Понятие роли. Использование ролевого принципа в рамках СУИБ. Преимущества использования ролевого принципа. Ролевая структура СУИБ (основные и дополнительные роли). Роль высшего руководства организации в СУИБ. Этапы разработки и функционирования СУИБ, на которых важно участие руководства организации. Суть участия руководства организации на этих этапах (утверждение документов, результатов анализа рисков и т.д.). Политика СУИБ. Понятие Политики СУИБ. Цели Политики СУИБ. Структура и содержание Политики СУИБ. Источники информации для разработки Политики СУИБ. Основы управления рисками ИБ. Управление рисками ИБ. Основные определения и положения управление рисками ИБ. Цель процесса анализа рисков ИБ. Этапы и участники процесса анализа рисков ИБ. Анализ рисков ИБ. Методики анализа рисков ИБ. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации. Типы угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов. Оценка рисков ИБ. Планирование мер

	по обработке выявленных рисков ИБ. Утверждение результатов анализа рисков ИБ у высшего руководства. Использование результатов анализа рисков ИБ. Процессы управления ИБ. Основные процессы СУИБ. Обязательная документация СУИБ. Процессы «Управление документами» и «Управление записями» (цели и задачи процессов, входные/выходные данные, роли участников, обязательные этапы процессов, связи с другими процессами СУИБ). Процессы улучшения СУИБ («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»). Процесс «Мониторинг эффективности» (включая разработку метрик эффективности). Понятие «Зрелость процесса». Процесс «Анализ со стороны высшего руководства». Процесс «Обучение и обеспечение осведомленности». Внедрение разработанных процессов. Документ «Положение о применимости». Этапы внедрения процессов и их последовательность. Обучение сотрудников, как один из этапов внедрения. Сложности, возникающие при внедрении процессов управления ИБ, и способы их решения. Контроль над внедрением процессов. Документирование процесса внедрения разработанных процессов. Типовой документ «Положение о применимости». Цель документа. Структура и содержание документа. Процесс разработки документа, решение спорных ситуаций при разработке документа. Внедрение мер (контрольных процедур) по обеспечению ИБ. Категории контрольных процедур. Перечень контрольных процедур по обеспечению ИБ в соответствии с лучшими международными практиками. Содержание контрольных процедур по обеспечению ИБ в интерпретации лучших практик. Процесс «Управление инцидентами ИБ». Цели и задачи процесса «Управления инцидентами ИБ, важность процесса с точки зрения управления ИБ Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ. Процесс «Обеспечение непрерывности ведения бизнеса». Цели и задачи процесса «Обеспечение непрерывности ведения бизнеса». Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ. Эксплуатация и независимый аудит СУИБ. Ввод системы в эксплуатацию. Возможные проблемы и способы их решения. Внешние аудиты ИБ на соответствие требованиям нормативных документов. Этапы проведения аудита ИБ. Результаты аудита ИБ и их интерпретация. Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. Законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ (авторское право, защита персональных данных и т.д.). Разработка процессов или
--	--

	дополнение существующих процессов управления ИБ с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены).
Результаты освоения дисциплины	- оперирует основными нормативными правовыми актами в области обеспечения информационной безопасности; нормативными методическими документами ФСБ России в области защиты информации; - разрабатывает проекты нормативных материалов, регламентирующих работу по защите информации, нормативно-методические материалы по регламентации системы организационной защиты информации, организационно-распорядительную документацию по обеспечению информационной безопасности; - Выделяет правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, стоимости и сроков реализации; - анализирует экономическую информацию, возникающую в процессе производственно-хозяйственной деятельности, и вырабатывает рекомендации по экономической целесообразности ее защиты, анализировать и классифицирует риски, возникающие при защите информации, выбирает методы их расчётов
Трудоемкость, з.е.	5
Форма отчетности	Экзамен, курсовая работа
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Поздняк, И. С. Управление информационной безопасностью : методические указания / И. С. Поздняк, И. С. Макаров. — Самара : ПГУТИ, 2019. — 43 с. 2. Поздняк, И. С. Планирование и управление информационной безопасностью : учебное пособие / И. С. Поздняк, И. С. Макаров, Л. Р. Чупахина. — Самара : ПГУТИ, 2020. — 69 с.
Дополнительная литература	1. Галатенко, В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. - Изд. 3-е. - М. : Интернет-Университет Информационных Технологий, 2005. - 208 с. - ISBN 5-9556-0052-3. - URL:http://biblioclub.ru/index.php?page=book&id=233063 2. Астахов, А.М. Искусство управления информационными рисками [Электронный ресурс] / А.М. Астахов. - М. : ДМК Пресс, 2010. - 312 с. - ISBN 978-5-94074-574-7. - URL:http://biblioclub.ru/index.php?page=book&id=86481 3. Анисимов, А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А.А. Анисимов. - М. : Интернет-Университет Информационных Технологий, 2009. - 176 с. - ISBN 9778-5-9963-0237-6. - URL:http://biblioclub.ru/index.php?page=book&id=232981 4. Минаев В.А., Фисун А.П. Правовое обеспечение

	информационной безопасности, Москва, 2008 г. – 368 с. 5. Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение информационной безопасности. – М.: Академия, 2008 г. – 192 стр.
--	--